1-1-2016

An empirical assessment of employee cyberslacking in the public sector: The social engineering threat

Wilnelia Hernández
Nova Southeastern University, wilnelia@nova.edu

Yair Levy
Nova Southeastern University, levyy@nova.edu

Michelle M. Ramim
Middle Georgia State University, michelle.ramim@mga.edu

Online Journal of Applied Knowledge Management
A Publication of the International Institute for Applied Knowledge Management

Volume 4, Issue 2, 2016

An empirical assessment of employee cyberslacking in the public sector: The social engineering threat

Wilnelia Hernández, Nova Southeastern University, wilnelia@nova.edu

Yair Levy, Nova Southeastern University, levyy@nova.edu

Michelle M. Ramim, Middle Georgia State University, michelle.ramim@mga.edu

Abstract

Employees spend time during work hours on non-work related activities including visiting e-commerce Websites, managing personal email accounts, and engaging in e-banking. These types of actions in the workplace are known as cyberslacking. Cyberslacking affects employees' productivity, presents legal concerns, and undermines the security of the employer's network. This research study addressed the problem of cyberslacking in the public sector, by assessing the ethical severity of cyberslacking activities, as well as how employees perceived that the frequency of such activities occurred by their co-workers. Participants from public sector agencies were asked to report about their amount of time spent and frequency of cyberslacking, what they report about their co-workers' amount of time spent and frequency of cyberslacking, as well as their perceived ethical severity of cyberslacking in the workplace. Comparisons of the measures were also conducted. Results from 183 participants indicate that employees report their co-workers to engage in cyberslacking significantly higher than what they reported about themselves, while ethical severity of cyberslacking was not considered to be high. Discussions and implications for future research are provided.

Keywords: cyberslacking, cybersecurity, social engineering threat, public sector, ethical severity, employee productivity at work, information security threat vector for public organizations

Introduction

The implementation of a new strategic work process and the integration of a new electronic environment in the workplace, presents new challenges for employees in the 21st century (Kidwell, 2010). The incorporation of Internet technologies, computer technologies, information systems (IS), and, the misuse of those technologies, are on the rise daily (D'Arcy & Hovav, 2008; D'Arcy, Hovav, & Galetta, 2009; Wheatherbee, 2010). Mills, Hu, Beldona, and Clay (2001) defined *misuse* as "Cyberslacking, cyberloafing, and cyberbludging" (p. 34). According to Whitty and Carr (2006), "Cyberslacking is the overuse of the Internet in the workplace for purposes other than work" (p. 238). Cyberslacking at the workplace included spending work hours to shop online, visiting pornographic Websites, accessing social networking sites (SNS) for personal use, and utilizing the work computer to manage personal data just to name a few (Henle & Blanchard, 2008; Johnson & Indvik, 2003; Kidwell, 2010; Lara, Tacoronte, & Ding, 2006; Lim & Teo, 2005). Evidently, cyberslacking diminishes productivity in the workplace in both the governmental and private spheres. Thus, its proliferation in the workplace, in public

sector organizations, warrants investigation (Whitty & Carr, 2006). This exploratory study was set to provide an assessment of what employees report about their engagement in cyberslacking, but also report about their co-workers' misuse, along with assessing their perceived ethical severity of IS misuse. Comparisons between the measures were conducted.

Review of Literature

Cyberslacking at work has been reported to be on the rise (Ínce &, Gül, 2011). Moreover, cyberslacking has been compared to the use of the telephone for personal purpose when it was first introduced, resulting in reduced productivity at the workplace (Odlyzko, 2001;Manross, & Rice, 1986). It appears that the use of computing resources at the workplace has created a paradox. On one hand computer resources (i.e. the Web, email, social networking sites) have provided employees with ways to increase productivity, fulfill business processes with higher efficiency, on the other hand, such resources have provided opportunities for cyberslacking (Strader, Simpson, & Clayton, 2009; Johnson & Rawlins, 2008). Subsequently, cyberslacking concerns have put employers at risk for the integrity and security of their e-mail system as well as networks (Hardy, 2003; Kraemer-Mbula, Tank & Rush, 2013). Employees visiting unsecure Websites, downloading malicious file attachments, engaging in online gaming can potentially cause loss of trade secrets, breach of confidentiality, as well as breach of network security. Employees engaging in gaming, visiting pornographic Websites, watching content on YouTube can potentially place heavy demand on computer resources and bandwidth, as well as create liability exchanging inappropriate content (Oswalt, & Elliott-Howard, 2003).

Research Methodology

This research study was exploratory in nature using the proposed model indicated in Figure 1. This research study measured the self-reported cyberslacking activity frequency (SCAF), co-workers cyberslacking activity frequency (CCAF), self-reported cyberslacking activity time (SCAT), co-workers cyberslacking activity time (CCAT), and perceived ethical severity of cyberslacking activities (ESCA), both self-reported and reported about that of co-workers. Cyberslacking behaviors that was surveyed using a collection of activities indicated in prior literature, such as: shopping online during work hours, perusing pornographic sites, visiting SNS for personal use, and using work computers for managing personal data (Henle & Blanchard, 2008; Johnson & Indvik, 2003; Kidwell, 2010; Lara et al., 2006; Lim & Teo, 2005; Mills et al., 2001; Vitak et al., 2011; Websense, 2006).

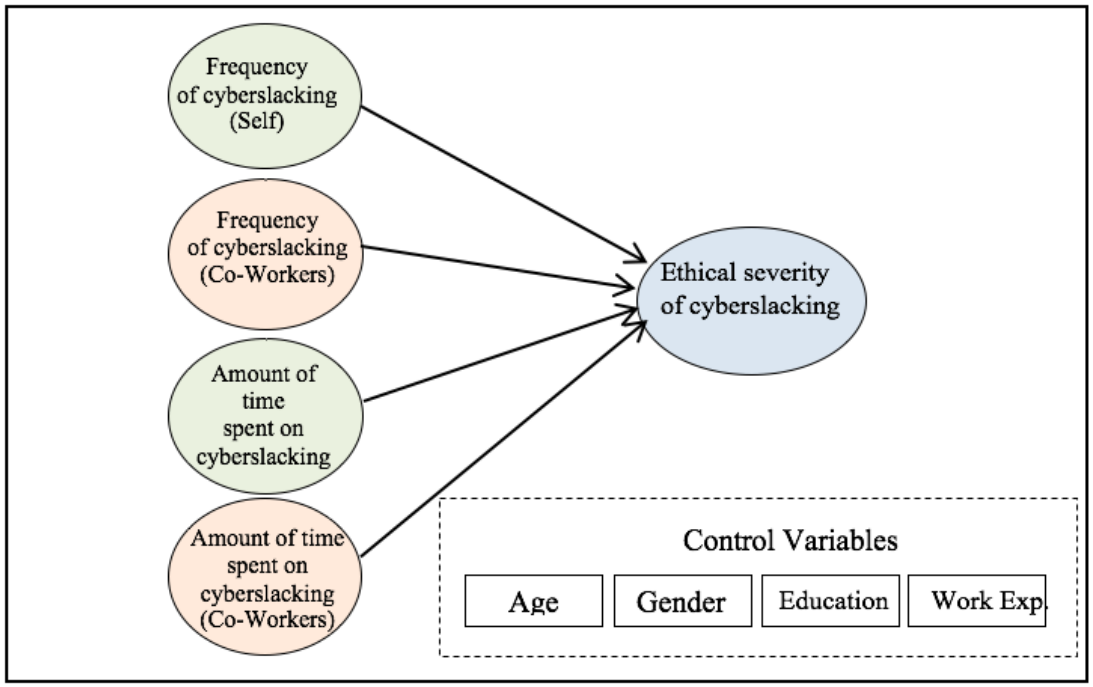

Figure 1. Conceptual Model on the Impact of Frequency and Amount of Time Spent on Cyberslacking on Ethical Severity of Such Activities

The frequency of participants' cyberslacking activities was reviewed from prior literature (Akman & Mishra, 2009; Blanchard & Henle, 2008; Magklaras & Furnell, 2005; Verton, 2000; Whitty, 2002; Whitty, 2004; Whitty & Carr, 2006). To measure frequency, the survey presented a 7-point Likert scale that included: 1=never, 2=once a month, 3=every other week, 4=once a week, 5=several days a week, 6=once a day, and 7=several times a day (Lim & Teo, 2005). According to each cyberslacking activity, participants selected their corresponding frequency of activity and the frequency of that of their co-workers corresponding to each of the activities.

To measure the amount of time spent on cyberslacking activities, this research study used a 7-point Likert scale based on the aforementioned literature. For amount of time spent, the scale included: 1=never, 2=on average about 15 minutes a day, 3=on average about 30 minutes a day, 4=on average about 1 hour a day, 5=on average about 2 to 4 hours a day, 6=on average about 5 to 7 hours a day, and 7=on average 8 or more hours a day. According to each cyberslacking activity, participants selected their corresponding amount of time spent on each activity and the amount of time that they perceived their co-workers spent on each cyberslacking activity.

The measure of perceived ethical severity of cyberslacking activities was reviewed and proposed based on prior literature (Oswalt et al., 2003; Levy et al., 2013; Vitak et al., 2011). Each of the previously discussed 20 activities was divided and participants selected how ethically severe they considered each cyberslacking activity in the workplace during work hours (Block, 2001; Gattiker & Kelley, 1999; Johnson & Rawlins, 2008). To measure level of perceived ethical severity on each cyberslacking activity, the measure had a 7-point Likert scale following Levy et al. (2013), which include the scale of: 1=highly unethical, 2=unethical, 3=somewhat unethical, 4=neither, 5=somewhat ethical, 6=ethical, and 7=highly ethical. According to each cyberslacking

activity, participants will select their corresponding level of perceived ethical severity of each activity.

Study Participants

The participants in this research study were employees from several agencies of the Executive Branch of the Government of Puerto Rico. Participants were invited to participate in the study via email, noting that participation was voluntary. The sample includes individuals from government agencies, with different ages, genders, educational levels, job levels, and varying years of working for government. An online anonymous survey was distributed via e-mail. Moreover, the e-mail invitation to participate included an acknowledgement from the head of each agency in order to help increase participation rate in this research study.

Study Measures

This research study uses a quantitative survey instrument to collect the data (Sekaran, 2003). The survey instrument have six sections: (a) self cyberslacking activity frequency; (b) co-workers' cyberslacking activity frequency; (c) self cyberslacking activities time; (d) co-workers' cyberslacking activities time; (e) ethical severity of cyberslacking activities; and (f) demographic information. The term "cyberslacking activity" was noted on the survey as "cyber activity" to reduce user bias. The first four sections of the quantitative survey contained 20 cyberslacking activities (Henle & Blanchard, 2008; Johnson & Indvik, 2003; Kidwell, 2010; Lara et al., 2006; Lim & Teo, 2005). To assess the measured variables, the survey instrument items had a 7-point Likert scale to facilitate the participants identifying the activity and the perceived ethical severity respectively.

Cyberslacking Activities

The measure of frequency, time spent, and perceived ethical severity was based on 20 cyberslacking activities on which study participants were asked to report. Participants were asked to self-report their cyberslacking activity frequency, report their co-workers' cyberslacking activity frequency, self-report cyberslacking activities time, report their co-workers' cyberslacking activity time, and report their perceived ethical severity of the 20 cyberslacking activities (Blanchard & Henle, 2008; Henle & Blanchard, 2008; Johnson & Indvik, 2003; Kidwell, 2010; Kim & Byrne, 2011; Lara et al., 2006; Lim & Teo, 2005; Vitak et al., 2011). Table 1 outlines the list of the 20 cyberslacking activities found in prior literature that was used in this study measures.

Table 1. Cyberslacking Activities (CA)

Item	Cyberslacking activities	Item Source(s)
CA1	Check non-work related email	Blanchard & Henle, 2008; Kim & Byrne, 2011; Lara et al., 2006; Lim, 2002; Lim & Teo, 2005
CA2	Send non-work related email	Blanchard & Henle, 2008; Kim & Byrne, 2011; Lara et al., 2006; Lim, 2002; Lim & Teo, 2005; Vitak et al., 2011
CA3	Visit general news sites	Blanchard & Henle, 2008; Kidwell, 2010; Kim & Byrne, 2011; Lim, 2002; Lim & Teo, 2005
CA4	Visit stock or investment related Websites	Blanchard & Henle, 2008; Kim & Byrne, 2011; Lim, 2002; Lim & Teo, 2005
CA5	View sports-related Websites	Blanchard & Henle, 2008; Kim & Byrne, 2011; Lim, 2002; Lim & Teo, 2005
CA6	Visit banking- or finance-related Websites	Blanchard & Henle, 2008; Kim & Byrne, 2011; Lim, 2002
CA7	Shop online for personal goods	Blanchard & Henle, 2008; Kidwell, 2010; Kim & Byrne, 2011; Lim & Teo, 2005; Vitak et al., 2011
CA8	Visit online auctions sites (e.g., eBay)	Blanchard & Henle, 2008; Kim & Byrne, 2011
CA9	Send/receive instant messaging	Blanchard & Henle, 2008; Kim & Byrne, 2011; Lim & Teo, 2005; Vitak et al. 2011
CA10	Participate in online games	Blanchard & Henle, 2008; Kim & Byrne, 2011; Lim & Teo, 2005; Vitak et al., 2011
CA11	Participate in chat rooms	Blanchard & Henle, 2008; Kim & Byrne, 2011
CA12	Visit newsgroups or bulletin boards	Blanchard & Henle, 2008; Kim & Byrne, 2011
CA13	Book vacations/travel	Blanchard & Henle, 2008; Kim & Byrne, 2011
CA14	Visit virtual communities	Blanchard & Henle, 2008; Kim & Byrne, 2011
CA15	Maintain a personal Web page	Blanchard & Henle, 2008; Kidwell, 2010; Kim & Byrne, 2011
CA16	Download music	Blanchard & Henle, 2008; Kim & Byrne, 2011
CA17	Visit job-hunting or employment-related Websites	Blanchard & Henle, 2008; Kim & Byrne, 2011; Lim & Teo, 2005
CA18	Visit gambling Websites	Blanchard & Henle, 2008; Kim & Byrne, 2011
CA19	Read blogs	Blanchard & Henle, 2008; Kim & Byrne, 2011; Vitak et al., 2011
CA20	View sexually explicit Websites	Blanchard & Henle, 2008; Kim & Byrne, 2011; Lim, 2002; Lim & Teo, 2005

The main research question (RQ) that this research study addressed was: to what extent (i.e. amount of time spent & frequency) are government employees self-report about themselves and their co-workers on engagement in cyberslacking activities in the workplace. Additionally, how ethically severe they perceive these cyberslacking activities to be, as well as if there are any significant differences on these measures based on gender, age, level of education, and years of employment. The specific research questions that this research study addressed were:

RQ1: What is the government employees' self-reported *frequency of engagement* in cyberslacking activities?

RQ2: What is the government employees' reported *frequency of co-workers' engagement* in cyberslacking activities?

RQ3: What is the government employees' self reported amount of *time spent on engagement* in cyberslacking activities?
RQ4: What is the government employees' reported of *co-workers' amount of time spent on engagement* in cyberslacking activities?
RQ5: What is the government employees' perceived *ethical severity* of engagement in cyberslacking activities?
RQ6: Are there any significant differences in government employees' self-reported frequency of engagement in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government?
RQ7: Are there any significant differences in government employees' reported frequency of co-workers' engagement in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government?
RQ8: Are there any significant differences in government employees' self-reported amount of time spent engaging in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government?
RQ9: Are there any significant differences in government employees' reported the amount of time spent by co-workers engaging in cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government?
RQ10: What is the impact of government employees' self-reported amount of time spent (self + co-workers) and frequency of engagement (self + co-workers) in cyberslacking activities on their perceived ethical severity of such activities?

Results

Analysis

The pre-analysis data screening was conducted and 183 usable responses were available for the analyses. The data showed that 62 or 33.9% of the respondents were males and 121 or 66.1% were females, while 106 or 57.9% were between the ages of 40 to 59. In academic level, 67 or 36.6% of the respondents had bachelor's degree and 105 or 57.4% were not supervising other employees. The demographic details of the sample collected are presented in Table 2.

Table 2. Descriptive statistics of population (N=183)

Item	Frequency	Percentage (%)
Gender		
Male	62	33.9%
Female	121	66.1%
Age		
18 to 24	1	0.5%
25 to 29	12	6.6%
30 to 39	57	31.1%
40 to 49	63	34.4%
50 to 59	43	23.5%
60 to 64	6	3.3%
65 or older	1	0.5%
Academic Level		
None	0	0%
High school diploma	0	0%
Associates degree	12	6.6%
Bachelor's degree	67	36.6%
Master's degree	65	35.5%
Professional degree	9	4.9%
Doctoral degree	30	16.4%
Job Level		
Supervising	78	42.6%
No Supervising	105	57.4%
Years in Government		
1 or less years	1	0.5%
1 to 5 years	33	18.0%
6 to 10 years	29	15.8%
11 to 15 years	34	18.6%
16 to 20 years	27	14.8%
21 or more	59	32.2%

Reliability

This research study used Cronbach's Alpha to assess the reliability of each of the measured constructs. An acceptable valid Cronbach's Alpha for a construct is usually one that is over 0.7 (Sekaran, 2003). The Cronbach's Alpha for the five constructs measured demonstrated high reliability with: 0.967, 0.940, 0.933, 0.864, and 0.773 for ESCA, CCAT, CCAF, SCAT, and SCAF respectively.

In order to preform the analyses to address the research questions of this study, first data aggregation was conducted. Given the assumption that the items were linearly distributed, all five constructs were aggregated linearly following the Eq. 1 to Eq. 5 as noted below. Given that each item in each construct used a scale of 1-7, the range of the aggregated scores of the

constructs were from 20 to 140 (See Figure 2). Table 3 provides the means of the aggregated constructs scores for all five constructs: SCAF, SCAT, CCAF, CCAT, and ESCA.

Eq. 1: $SCAF = SCAF_1 + SCAF_2 + \ldots. + SCAF_{20}$
Eq. 2: $CCAF = CCAF_1 + CCAF_2 + \ldots. + CCAF_{20}$
Eq. 3: $SCAT = SCAT_1 + SCAT_2 + \ldots. + SCAT_{20}$
Eq. 4: $CCAT = CCAT_1 + CCAT_2 + \ldots. + CCAT_{20}$
Eq. 5: $ESCA = ESCA_1 + ESCA_2 + \ldots. + ESCA_{20}$

Table 3. Results of the Means of the Aggregated Constructs Scores for all Five Constructs (N=183)

Constructs	Means of the Aggregated Constructs Scores	Standard Deviation
SCAF	32.77	11.95
CCAF	43.36	24.59
SCAT	25.42	8.37
CCAT	31.79	14.71
ESCA	43.83	23.05

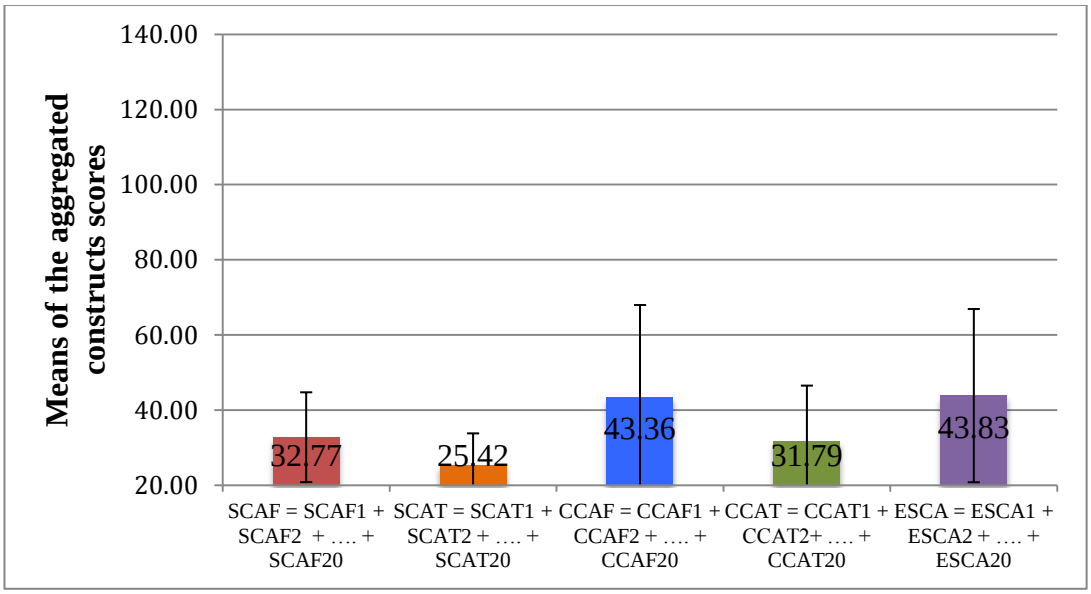

Figure 2. Means of the Aggregated Constructs Scores for all Five Constructs

This research study used analysis of covariance (ANCOVA) to answer RQ7-RQ9. According to Mertler and Vannatta (2012), ANCOVA was used to analyze the differences when controlled by the demographic indicators. The ANCOVA is similar to ANOVA, but Mertler and Vannatta (2012) stated, "ANCOVA additionally controls for a variable (covariate) that may influence the

DV" (p. 15). Tables 4, 6, 7, and 8 present an overview of the ANCOVA analyses of the demographic indicators for SCAF, CCAF, SCAT, and CCAT with ESCA as dependent variable.

Table 4. Analysis of the Covariance of SCAF with ESCA as Dependent Variable (N=183)

	ANCOVA of SCAF		
Demographics	**F**	**Sig.**	
Gender	3.63	.059	
Age	.594	.442	
Education	1.108	.294	
Job Level	1.336	.250	
Years in Government	.477	.491	

*- p<0.05, ** - p<0.01, *** - p<0.001

Table 5. Analysis of the Covariance of CCAF with ESCA as Dependent Variable (N=183)

	ANCOVA of CCAF		
Demographics	**F**	**Sig.**	
Gender	5.286	***.023***	*
Age	.013	.909	
Education	.407	.525	
Job Level	4.138	***.044***	*
Years in Government	1.555	.215	

* - p<0.05, ** - p<0.01, *** - p<0.001

Table 6. Analysis of the Covariance of SCAT with ESCA as Dependent Variable (N=183)

	ANCOVA of SCAT	
Demographics	**F**	**Sig.**
Gender	3.825	.052
Age	.446	.505
Education	2.807	.096
Job Level	.890	.347
Years in Government	1.337	.249

* - p<0.05, ** - p<0.01, *** - p<0.001

Table 7. Analysis of the Covariance of CCAT with ESCA as Dependent Variable (N=183)

ANCOVA of CCAT			
Demographics	**F**	**Sig.**	
Gender	6.326	***.013***	*
Age	.001	.969	
Education	.811	.369	
Job Level	2.878	.092	
Years in Government	1.379	.242	

* - p<0.05, ** - p<0.01, *** - p<0.001

Multiple Linear Regression (MLR)

Multiple Linear Regression (MLR) was used to answer the research question RQ10. Mertler and Vannatta (2012) stated that, "Multiple regression identifies the best combination of predictors (IVs) of the dependent variable [DV]" (p. 14). The regression equation was used to make the predictions of the ESCA construct (Sprinthall, 2007). In order to preform the MLR analysis, data aggregation previously done was used here as well based on the linear means scoring, given that the data demonstrated both acceptable normality and linearity. The result for predicting the DV (ESCA) from the four IV predictors (SCAF, SCAT, CCAF, & CCAT) was found that SCAT was the only significant (p<0.01) IV, with a positive regression weight. This result presents that ESCA increases significantly as scores on SCAT increases. Furthermore, SCAF, CCAF, and CCAT were not significant predictors of ESCA, however, it appears that CCAT was borderline, and may require further investigation, especially as it has a negative coefficient. Table 8 provides an overview of the MLR with the coefficients and significance.

Table 8. Multiple Linear Regression (MLR) Analysis Results (N=183)

Coefficients						
Model		**Unstandardized Coefficients**		**Standardized Coefficients**		
		B	Std. Error	Beta	T	Sig.
1	(Constant)	21.595	5.608		3.851	.000
	SCAF	.071	.207	.037	0.346	.730
	SCAT	.876	.287	.318	3.056	*.003*
	CCAF	.158	.129	.168	1.224	.223
	CCAT	-.290	.211	-.185	-1.375	.171

* - p<0.05, ** - p<0.01, *** - p<0.001

The portion of the variance in ESCA that was explained by SCAF, SCAT, CCAF, and CCAT in combination was $R^2 = 0.111$, or 11.1%, which appears to be very low. The results showed that CCAT have the more significance value with a solid coefficient value. In the opposite side, the

results showed that CCAT have a negative B coefficient with no significance, which means that as CCAT increases, the value of ESCA decreases, but non significantly.

Ordinal Logistic Regression (OLR)

Ordinal Logistic Regression (OLR) was also made to test the prediction of the dependent variable (ESCA) based on the four independent variables (SCAF, SCAT, CCAF, & CCAT) using non-linear regression. The results are consistent with the results of the MLR analysis. The OLR showed that SCAF (p=0.08) and SCAT (p=0.03) were significant. The overall model for predicting ESCA based on the four predictors (SCAF, SCAT, CCAF, & CCAT) showed: -2 Log Likelihood = 1371.767, $x^2(4) = 28.650$ p<0.001. Table 9 provides an overview of the OLR Model Significance. The result shows that it is very significance with a value of p<.001.

Table 9. Ordinal Logistic Regression Model Significance (N=183)

Model	-2Log Likelihood	Chi-Square	df	Sig.
Intercept Only	1371.767			
Final	1343.117	28.650	4	*.000* ***

* - p<0.05, ** - p<0.01, *** - p<0.001

The results of the OLR analysis showed that only two predictors (SCAF & SCAT) are significant and this indicated that these independent variables were significant predictors of ESCA. The results indicated that ESCA increase as scores of SCAF and SCAT increase. The negative value of CCAT indicated that higher scores on CCAT result on lower scores on ESCA. Table 10 provides an overview of the results of the OLR Parameter Estimates.

Table 10. Ordinal Logistic Regression (OLR) Parameter Estimates

	Estimate	Std. Error	Wald	df	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
SCAF	0.029	0.016	3.056	1	***0.08 ****	-0.003	0.061
SCAT	0.05	0.023	4.731	1	***0.03 ****	0.005	0.096
CCAF	0.01	0.01	1.024	1	0.311	-0.01	0.03
CCAT	-0.018	0.017	1.115	1	0.291	-0.05	0.015

* - p<0.05, ** - p<0.01, *** - p<0.001

Findings

This research study addressed the 10 research questions noted above. To answer the RQ1-RQ6 we used the results of the means of the aggregated of constructs scores for all five constructs and the standard deviation for each one. Table 11 showed the results corresponded to each question.

Table 11. Results of the Means of the Aggregated Constructs Scores for all Five Constructs

Constructs	Means of the Aggregated Constructs Scores	Standard Deviation
SCAF	32.77	11.95
CCAF	43.36	24.59
SCAT	25.42	8.37
CCAT	31.79	14.71
ESCA	43.83	23.05

Also, the results presented that there are no significant differences in government employees' self-reported frequency of engagement in cyberslacking activities based on gender, age, level of education, job level, and years working for government. This research study used ANCOVA to analyze the differences when controlled by the demographic indicators as noted in RQ7-RQ11. The result presented that there are significant differences in government employees reported frequency of co-workers' engagement in cyberslacking activities based on gender with p=0.023 and job level with p=0.044. Furthermore, there were no significant differences in government employees self-reported amount of time spent engaging in cyberslacking activities based on gender, age, level of education, job level, and years working for government. Also, there were significant differences in government employees' reported amount of time spent by co-workers engaging in cyberslacking activities based on gender with p=0.013. Finally, the results showed that there are a very significant differences in government employees perceived ethical severity of cyberslacking activities based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government. There are significant differences in government employees' perceived ethical severity of cyberslacking activities based on (a) gender and (d) job level on CCAF (See Table 6), as well as based on (a) gender on CCAT (See Table 8). MLR analysis shows that there are inverse relationship between ESCA and the SCAT. SCAT is the most influential IV with a significance level of p=0.003. The coefficient value of SCAF is negligible that result in non-significance. OLR analysis shows that SCAF and SCAT are significant predictors of ESCA. The result of SCAF is not too far from SCAT like in MLR. The strongest coefficient is SCAT with a significance of p=0.03 and the second strongest coefficient is SCAF with a significance of p=0.08. CCAT is negative coefficient with none significance which means that the more they report the more less ethical they are. The coefficient of CCAF is negligible that result in none significance.

Looking at the data in terms of SCAF the four activities that are the most frequent are: visit general news Websites, check non-work related e-mails, visit banking or finance-related Websites, and send non-work related e-mails. In terms of CCAF the four activities that are the most frequent are: visit general news sites, check non-work related e-mail, send non-work related e-mail, and visit banking or finance-related Websites. In terms of SCAT the four activities that employees spent more time are: visit general news sites, check non-work related e-mail, send non-work related e-mail, and send/receive instant messaging. Finally, in terms of CCAT the four

activities that employees spent more time are: visit general news sites, check non-work related e-mail, send non-work related e-mail, and visit banking or finance-related Websites.

Conclusions, Implications, and Future Research

A set of 10 research questions was addressed and implications of this study are highlighted. The contributions of this study to the IS body of knowledge by empirically identifying the role of amount of time spent and frequency of cyberslacking on individuals' perceived ethical severity of IS in the workplace are presented. The main goal of this proposed research study was to measure the self-reported extent (i.e. amount of time spent & frequency) to which government employees and their co-workers engage in cyberslacking activities in the workplace, to ascertain the perceived ethical severity of these cyberslacking activities, and to investigate if there are any differences on these measures based on (a) gender, (b) age, (c) level of education, (d) job level, and (e) years working for government. The sample of this study was 183 government employees of different agencies.

The results presented that there are no significant differences in government employees' self-reported frequency of engagement in cyberslacking activities based on gender, age, level of education, job level, and years working for government. MLR was found to be not significant and OLR was found to be significant. In MLR, only SCAT was significant with a value of $p<0.01$. This result shows that if SCAT has a high coefficient value ESCA has a lower value. In OLR model the result shows that SCAF and SCAT are significant IVs in the prediction of ESCA.

This research study has significant implications as a consequence of the massive increase in Internet-based tools in the workplace that area readily available to employees. According to Gottfredson and Hirschi (1990), "the theory of crime has implications for how crime itself is construed, how it should be measured, the kind of people who are likely to engage in it, and the institutional context within which it is controlled" (p. 4). They explained that there are two key factors for predicting criminal behavior: self-control opportunity and the second one is the opportunity (Gottfredson & Hirschi, 1990). These lacks of self-control occur when employees engage in the misuse of Web tools in the workplace (Kim & Byrne, 2011). This investigation contribute to the IS body of knowledge by empirically identifying the role of amount of time spent and frequency of cyberslacking on individuals' perceived ethical severity of IS in the workplace.

This study presented a limitation with the generalizability of the sample. The participants in this research study represented only several agencies of the Executive Branch of the Government of Puerto Rico. According to Oswalt et al. (2003), the distraction of Internet presents an ethical issue in the workplace. Another limitation was that agencies do not want that their employees participate in this type of study because they admit that their employees are engage in cyberslacking activities. Houston and Tran (2001) stated that, "the problem facing researchers is how to encourage participants to respond, and then to provide a truthful response in surveys. This is another limitation of this study, truthful response in surveys" (p. 70). The bureaucracy of the process in the government to participate in this type of research study was another limitation. Furthermore, unions in government agencies were posing another limitation, because several

agencies do not want to exposed their employees to this type of study. Finally, the quantity of questions in the survey was another limitation.

Nowadays, Internet services are essential components of the underlying infrastructure of organizations (Whitty & Carr, 2006). According to Mills et al. (2001), "Companies have developed an Internet acceptable-use policy (IAUP)" (p. 47). With an IAUP, a company establishes the policy for correct use of Internet technologies in the workplace, which, in conjunction with the enforcement controls implemented, can result in control over employees' use of those resources.

There are many areas for future research that were identified based on the results of this investigation. The first recommendation is that this investigation could be replicated with a short version of the survey. The second recommendation is to replicate the survey with cyberslacking activities of using personal mobile devices. The third recommendation for future research study is to determine the impact of government employees' *reported amount of time spent* (self + co-workers) and *frequency* of engagement (self + co-workers) in cyberslacking activities of their *perceived cyber security severity* of such activities.

References

Akman, I., & Mishra, A. (2009). Ethical behavior issues in software use: An analysis of public and private sectors. *Computers in Human Behavior, 25*(6), 1251-1257.

Blanchard, A., & Henle, C. (2008). Correlates of different forms of cyberloafing: The role of norms and external locus of control. *Computers in Human Behavior, 24*(3), 1067-1084.

Block, W. (2001). Cyberslacking, business ethics and managerial economics. *Journal of Business Ethics, 33*(3), 225-231.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence perspective. *Information Systems Research*, *20* (1), pp. 79-98.

Floyd J., & Fowler, Jr. (1995). *Improving survey questions design and evaluation.* Massachusetts, BSN: SAGE Publications, Inc.

Gattiker, U., & Kelley, H. (1999). Morality and computers: Attitudes and differences in moral judgments. *Information Systems Research*, *10*(3), 233-254.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford, CA: Stanford University Press.

Hardy, H. E. (2003). Internet, history and development of. *Encyclopedia of International Media and Communications, Volume 2*.

Henle, C. A., & Blanchard, A. L. (2008). The interaction of work stressors and organizational sanctions on cyberloafing. *Journal of Managerial Issues*, *20*(3), 383-400.

Houston, J., & Tran, A. (2001). A survey of tax evasion using the randomized response technique. *Advances in taxation, 13,* 69–94.

Ínce, M., & Gül, H. (2011). The relation of cyber slacking behaviors with various organizational outputs: Example of Karamanoğlu Mehmetbey University. *European Journal of Scientific Research*, *52*(4), 507–527.

Oswalt, B., & Elliott-Howard, F. (2003). Cyberslacking – Legal and ethical issues facing IT managers. Retrieved Februry 12, 2016, from iacis.org

Johnson, P. R., & Indvik, J. (2003). The organizational benefits of reducing cyberslacking in the workplace. *Journal of Organizational Culture, Communications, and Conflict*, *8*(2), 55−62.

Johnson, P. R., & Rawlins, C. (2008). Employee internet management: Getting people back to work. *Journal of Organizational Culture, Communications, and Conflict*, *12*(1), 43-49.

Kidwell, R. E. (2010). Loafing in the 21st century: Enhanced opportunities -- and remedies -- for withholding job effort in the new workplace. *Business Horizons*, *53*(6), 543-552.

Kim, S. J., & Byrne, S. (2011). Conceptualizing personal web usage in work contexts: A preliminary framework. *Computers in Human Behavior*, *27*(6), 2271-2283.

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, *80*(3), 541–555.

Lara, P. Z., Tacoronte, D. V., & Ding, J. T. (2006). Do current anti-cyberloafing

disciplinary practices have a replica in research findings?: A study of the effects of coercive strategies on workplace Internet misuse. *Internet Research*, *16*(4), 450-467.

Levy, Y., Ramim, M. M., & Hackney, R.A. (2013). Assessing ethical severity of e-learning systems security attacks. *Journal of Computer Information Systems*, *53*(3), 75-84.

Lim, V., & Teo, T. (2005). Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: An exploratory study. *Information & Management*, *42*(8), 1081-1093.

Magklaras, G. B., & Furnell, S. M. (2005). A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security*, *24*(5), 371-380.

Manross, G. G., & Rice, R. E. (1986). Don't hang up: Organizational diffusion of the intelligent telephone. *Information & Management*, *10*(3), 161-179.

Mertler, C., & Vannatta, R.A. (2012). *Advanced and multivariate statistical methods: Practical application and interpretation (5th ed.)*. Glendale, CA:Pyrczak Publishing.

Mills, B. Y., Hu, B. O., Beldona, S., & Clay, J. (2001). Cyberslacking! *Cornell Hotel and Restaurant Administration Quarterly*, 34-47.

Odlyzko, A. (2001). Internet pricing and the history of communications. *Computer Networks*, *36*(5-6), 493–517.

Oswalt, B., Florence, E.H., & Austin, S. F. (2003). Cyberslacking -- legal and ethical issues. *International Association for Computer Information Systems* (pp. 646-652).

Sekaran, U. (2003). *Research methods for business. A skill building approach (4th ed.).* New York, NY: John Wiley and Sons.

Sekaran, U. (2013). *Research methods for business. A skill building approach (6th ed.).* New York, NY: John Wiley and Sons.

Straub, D. W. (1989). Validating instruments in MIS Research. *MIS Quarterly*, *13*(2), 147-169.

Weatherbee, T. G. (2010). Counterproductive use of technology at work: Information & communications technologies and cyberdeviancy. *Human Resource Management Review*, *20*(1), 35-44.

Verton, D. (2000). Employers ok with e-surfing. *Computerworld*, *34*(1), 16.

Vitak, J., Crouse, J., & LaRose, R. (2011). Personal Internet use at work: Understanding cyberslacking. *Computers in Human Behavior*, *27*(5), 1751-1759.

Websense, Inc. Web@Work (2006). Retrieved August 20, 2011, from http://www.securitymanagement.com/archive/library/websense_technofile0906.pdf.

Whitty, M. T. (2002). Big brother in Australia: Privacy and surveillance of the Internet in the Australian workplace. *Internet Research 3.0: Net/Work/Theory*, Netherlands.

Whitty, M. T. (2004). Should filtering software be utilized in the workplace? Australian employees' attitudes towards Internet usage and surveillance of the Internet in the workplace. *Surveillance and Society, 2*(1), 39–54.

Whitty, M. T., & Carr, A. N. (2006). New rules in the workplace: Applying object-relations theory to explain problem Internet and email behavior in the workplace. *Computers in Human Behavior, 22*, 235-250.

Authors' Biographies

Wilnelia Hernández, Ph.D. is the Director of IS at *Universidad del Turabo* in Puerto Rico. She received her Ph.D. in Information Systems from the College of Engineering and Computing at Nova Southeastern University. She also holds a Master in Business Administration with a concentration in Technology Management. Also, she holds a Bachelor's of Science degree in Computational Mathematics from the University of Puerto Rico. She has worked in the technology industry for 17 years, holding several positions including a professor position at the college of *Instituto de Banca y Comercio de Puerto Rico* and System Analyst at the *Oficina de Ética Gubernamental de Puerto Rico*. Dr. Hernandez's research interests include Cyberslacking, Ethics in Computer Science, Cybersecurity, Privacy in Information Systems, among others. She has participated and published in several conference proceedings. Also, she has served as a reviewer in several conferences including IEEE SoutheastCon 2015, Knowledge Management Conference 2014, and 2015.

Yair Levy, Ph.D. is a Professor of Information Systems and Cybersecurity at the College of Engineering and Computing, at Nova Southeastern University, the Director of the Center for e-Learning Security Research (CeLSR), and chair of the Information Security Faculty Group at the college. He joined the university in 2003, was promoted to an Associate Professor in 2007, and to full Professor in 2012. During the mid to late 1990s, Dr. Levy assisted NASA to develop e-learning platforms as well as manage Internet and Web infrastructures. He earned his undergraduate degree in Aerospace Engineering from the Technion (Israel Institute of Technology). He received his Masters of Business Administration (MBA) with Management Information Systems (MIS) concentration and Ph.D. in MIS from Florida International University. He heads the Levy CyLab, which conducts innovative research from the human-centric lens of four key research areas Cybersecurity, User-authentication, Privacy, and Skills (CUPS), as well as their interconnections. He authored over 60 articles, three book chapters, one book, and his publications have been cited for over 1,400 times by other scholarly research. Dr. Levy has been an active member of the US Secret Service (USSS)'s - Miami Electronic Crimes Task Force (MECTF). He was trained by the Federal Bureau of Investigation (FBI) on various topics, and actively serves as a member of the FBI/InfraGard, and consults the FBI/Cyber Task Force (CTF). Dr. Levy serves on the national Joint Task Force of Cybersecurity Education, as

well as other national initiatives related to cybersecurity workforce, education, and research. He is also a frequent invited keynote speaker at national and international meetings, as well as regular media interviews as a Subject Matter Expert (SME) on cybersecurity topics. Find out more about Dr. Levy and his research lab via: http://cec.nova.edu/~levyy/

Michelle M. Ramim, Ph.D. is a part-time professor at the Middle Georgia State University. She has extensive experience in information technology (IT) consulting. Dr. Ramim directed the development and implementations of several IT projects including promotional and interactive websites for major enterprises such as Debeer (Diamond Trading Company). Her current research interests include ethical issues with IT, information security and crisis management, privacy and legal aspects of computing, as well as ethical decision making. She has published articles in peer-reviewed outlets including journals, conference proceedings, encyclopedias, and an invited chapter. A number of her papers won the 'best paper' award in national and international peer-review conference proceedings. Moreover, she has been serving as a referee reviewer for national and international scientific journals, conference proceedings, as well as management information systems textbooks. She has developed the supplemental material for the Pearlson and Saunders (2012) 5th ed. Book "Managing and Using Information Systems: A Strategic Approach" by Wiley & Sons. She earned her Bachelor's degree from Barry University in Miami, Florida. Dr. Ramim has received her Executive MBA from Florida International University. She completed her Ph.D. in Information Systems at the College of Engineering and Computing, Nova Southeastern University.